**MALICIOUS**

Classifications: Injector | Spyware | Backdoor | Keylogger

Threat Names: Quasar | xRAT | QuasarRAT | AZORult | Trojan.GenericKD.41182905 | Trojan.GenericKD.44524794 | Trojan.GenericKD.43426068 | Gen:Variant.Fugrafa.7193 | Gen:Variant.Graftor.774294 | Generic.Delph.PWS.D0207221 | Gen:Variant.Razy.681395 | Trojan.PWS.ZNN

Verdict Reason: -

| | |
|---|---|
| **Sample Type** | **Windows Exe (x86-32)** |
| **File Name** | **efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe** |
| ID | #2782920 |
| MD5 | b0b78da613422be0de8de2e2a2d0ce68 |
| SHA1 | a1aea30e16b3bbf15baf1fbb78499adcc5e11d97 |
| SHA256 | efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0 |
| File Size | 2061.78 KB |
| Report Created | 2021-09-28 14:14 (UTC+2) |
| Target Environment | win10_64_th2_en_mso2016 \| exe |

# OVERVIEW

## VMRay Threat Identifiers (33 rules, 164 matches)

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 5/5 | YARA | Malicious content matched by YARA rules | 22 | Backdoor, Spyware |

- Rule "QuasarRATCommands_1_3" from ruleset "RATs" has matched on the dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe".
- Rule "Quasar_RAT_2" from ruleset "RATs" has matched on the dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe".
- Rule "xRAT_1" from ruleset "RATs" has matched on the dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe".
- Rule "xrat_quasarrat" from ruleset "RATs" has matched on the dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe".
- Rule "QuasarRATCommands_1_3" from ruleset "RATs" has matched on the sample itself.
- Rule "Quasar_RAT_2" from ruleset "RATs" has matched on the sample itself.
- Rule "xrat_quasarrat" from ruleset "RATs" has matched on the sample itself.
- Rule "QuasarRATCommands_1_3" from ruleset "RATs" has matched on the dropped file "C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe".
- Rule "Quasar_RAT_2" from ruleset "RATs" has matched on the dropped file "C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe".
- Rule "xrat_quasarrat" from ruleset "RATs" has matched on the dropped file "C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe".
- Rule "QuasarRATCommands_1_3" from ruleset "RATs" has matched on a memory dump for (process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe.
- Rule "Quasar_RAT_2" from ruleset "RATs" has matched on a memory dump for (process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe.
- Rule "xrat_quasarrat" from ruleset "RATs" has matched on a memory dump for (process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe.
- Rule "Azorult_Generic" from ruleset "Malware" has matched on a memory dump for (process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe.
- Rule "QuasarRATCommands_1_3" from ruleset "RATs" has matched on a memory dump for (process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe.
- Rule "Quasar_RAT_2" from ruleset "RATs" has matched on a memory dump for (process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe.
- Rule "xrat_quasarrat" from ruleset "RATs" has matched on a memory dump for (process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe.
- Rule "QuasarRATCommands_1_3" from ruleset "RATs" has matched on a memory dump for (process #3) windef.exe.
- Rule "Quasar_RAT_2" from ruleset "RATs" has matched on a memory dump for (process #3) windef.exe.
- Rule "xRAT_1" from ruleset "RATs" has matched on a memory dump for (process #3) windef.exe.
- Rule "xrat_quasarrat" from ruleset "RATs" has matched on a memory dump for (process #3) windef.exe.
- Rule "Azorult_Generic" from ruleset "Malware" has matched on a memory dump for (process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe.

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 4/5 | Defense Evasion | Obscures a file's origin | 3 | - |

- (Process #3) windef.exe tries to delete zone identifier of file "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe".
- (Process #3) windef.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe".
- (Process #11) winsock.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe".

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 4/5 | Injection | Writes into the memory of another process | 1 | Injector |

- (Process #2) vnc.exe modifies memory of (process #4) svchost.exe.

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 4/5 | Injection | Modifies control flow of another process | 1 | - |

- (Process #2) vnc.exe alters context of (process #4) svchost.exe.

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 4/5 | Antivirus | Malicious content was detected by heuristic scan | 14 | - |

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| | | • Built-in AV detected the dropped file C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe as "Trojan.GenericKD.44524794".<br>• Built-in AV detected the dropped file C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe as "Trojan.GenericKD.43426068".<br>• Built-in AV detected the sample itself as "Trojan.GenericKD.41182905".<br>• Built-in AV detected the sample itself as "AIT:Trojan.Nymeria.1811".<br>• Built-in AV detected the dropped file C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe as "Trojan.GenericKD.41182905".<br>• Built-in AV detected the dropped file C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe as "Trojan.GenericKD.44524794".<br>• Built-in AV detected the dropped file C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe as "Trojan.GenericKD.43426068".<br>• Built-in AV detected the dropped file C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe as "AIT:Trojan.Nymeria.1811".<br>• Built-in AV detected a memory dump of (process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe as "Gen:Variant.Fugrafa.7193".<br>• Built-in AV detected a memory dump of (process #2) vnc.exe as "Gen:Variant.Graftor.774294".<br>• Built-in AV detected a memory dump of (process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe as "Generic.Delph.PWS.D0207221".<br>• Built-in AV detected a memory dump of (process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe as "Gen:Variant.Fugrafa.7193".<br>• Built-in AV detected a memory dump of (process #4) svchost.exe as "Gen:Variant.Razy.681395".<br>• Built-in AV detected a memory dump of (process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe as "Trojan.PWS.ZNN". | | |
| 4/5 | Reputation | Known malicious file | 2 | - |
| | | • File "C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe" is a known malicious file.<br>• File "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe" is a known malicious file. | | |
| 3/5 | Input Capture | Monitors keyboard input | 1 | Keylogger |
| | | • (Process #11) winsock.exe installs system wide "WH_KEYBOARD_LL" hook(s) to monitor keystrokes. | | |
| 3/5 | Injection | Injects a file into another process | 66 | - |

- (Process #11) winsock.exe injects file into (process #14) claim.exe.
- (Process #11) winsock.exe injects file into (process #15) quite do.exe.
- (Process #11) winsock.exe injects file into (process #16) drop.exe.
- (Process #11) winsock.exe injects file into (process #17) that_but.exe.
- (Process #11) winsock.exe injects file into (process #18) knowledge sign.exe.
- (Process #11) winsock.exe injects file into (process #19) raiseleftbuy.exe.
- (Process #11) winsock.exe injects file into (process #20) clear.exe.
- (Process #11) winsock.exe injects file into (process #21) watch.exe.
- (Process #11) winsock.exe injects file into (process #22) whosouth.exe.
- (Process #11) winsock.exe injects file into (process #23) factor-western-forget.exe.
- (Process #11) winsock.exe injects file into (process #24) throwtowardpurpose.exe.
- (Process #11) winsock.exe injects file into (process #25) serve.exe.
- (Process #11) winsock.exe injects file into (process #26) weaponnatural.exe.
- (Process #11) winsock.exe injects file into (process #27) camera.exe.
- (Process #11) winsock.exe injects file into (process #28) nothing foreign.exe.
- (Process #11) winsock.exe injects file into (process #29) move.exe.
- (Process #11) winsock.exe injects file into (process #30) arrive.exe.
- (Process #11) winsock.exe injects file into (process #31) storypolice.exe.
- (Process #11) winsock.exe injects file into (process #32) include effect seven.exe.
- (Process #11) winsock.exe injects file into (process #33) scriptftp.exe.
- (Process #11) winsock.exe injects file into (process #34) icq.exe.
- (Process #11) winsock.exe injects file into (process #35) skype.exe.
- (Process #11) winsock.exe injects file into (process #36) notepad.exe.
- (Process #11) winsock.exe injects file into (process #37) leechftp.exe.
- (Process #11) winsock.exe injects file into (process #38) alftp.exe.
- (Process #11) winsock.exe injects file into (process #39) afr38.exe.
- (Process #11) winsock.exe injects file into (process #40) centralcreditcard.exe.
- (Process #11) winsock.exe injects file into (process #41) fling.exe.
- (Process #11) winsock.exe injects file into (process #42) bitkinex.exe.
- (Process #11) winsock.exe injects file into (process #43) absolutetelnet.exe.
- (Process #11) winsock.exe injects file into (process #44) foxmailincmail.exe.
- (Process #11) winsock.exe injects file into (process #45) trillian.exe.
- (Process #11) winsock.exe injects file into (process #46) filezilla.exe.
- (Process #11) winsock.exe injects file into (process #47) yahoomessenger.exe.
- (Process #11) winsock.exe injects file into (process #48) whatsapp.exe.
- (Process #11) winsock.exe injects file into (process #49) active-charge.exe.
- (Process #11) winsock.exe injects file into (process #50) operamail.exe.
- (Process #11) winsock.exe injects file into (process #51) ncftp.exe.
- (Process #11) winsock.exe injects file into (process #52) accupos.exe.
- (Process #11) winsock.exe injects file into (process #53) winscp.exe.
- (Process #11) winsock.exe injects file into (process #54) gmailnotifierpro.exe.
- (Process #11) winsock.exe injects file into (process #55) pidgin.exe.
- (Process #11) winsock.exe injects file into (process #56) outlook.exe.
- (Process #11) winsock.exe injects file into (process #57) smartftp.exe.
- (Process #11) winsock.exe injects file into (process #58) webdrive.exe.
- (Process #11) winsock.exe injects file into (process #59) ccv_server.exe.
- (Process #11) winsock.exe injects file into (process #60) creditservice.exe.
- (Process #11) winsock.exe injects file into (process #61) flashfxp.exe.
- (Process #11) winsock.exe injects file into (process #62) isspos.exe.
- (Process #11) winsock.exe injects file into (process #63) far.exe.
- (Process #11) winsock.exe injects file into (process #64) edcsvr.exe.
- (Process #11) winsock.exe injects file into (process #65) coreftp.exe.
- (Process #11) winsock.exe injects file into (process #66) mxslipstream.exe.
- (Process #11) winsock.exe injects file into (process #67) thunderbird.exe.
- (Process #11) winsock.exe injects file into (process #68) aldelo.exe.
- (Process #11) winsock.exe injects file into (process #69) spcwin.exe.
- (Process #11) winsock.exe injects file into (process #70) fpos.exe.
- (Process #11) winsock.exe injects file into (process #71) barca.exe.
- (Process #11) winsock.exe injects file into (process #72) iexplore.exe.
- (Process #11) winsock.exe injects file into (process #73) spagentservice.exe.

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 2/5 | Anti Analysis | Tries to detect debugger | 1 | - |
| | • (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe tries to detect a debugger via API "IsDebuggerPresent". | | | |
| 2/5 | Discovery | Queries OS version via WMI | 2 | - |
| | • (Process #3) windef.exe queries OS version via WMI.<br>• (Process #11) winsock.exe queries OS version via WMI. | | | |
| 2/5 | Discovery | Executes WMI query | 2 | - |
| | • (Process #3) windef.exe executes WMI query: SELECT Caption FROM Win32_OperatingSystem.<br>• (Process #11) winsock.exe executes WMI query: SELECT Caption FROM Win32_OperatingSystem. | | | |
| 2/5 | Discovery | Reads network adapter information | 2 | - |
| | • (Process #3) windef.exe reads the network adapters' addresses by API.<br>• (Process #11) winsock.exe reads the network adapters' addresses by API. | | | |
| 2/5 | Hide Tracks | Hides files | 2 | - |
| | • (Process #3) windef.exe hides the file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe" by setting its "hidden" attribute.<br>• (Process #11) winsock.exe hides the file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe" by setting its "hidden" attribute. | | | |
| 2/5 | Injection | Injects a file into a process started from a created or modified executable | 1 | - |
| | • (Process #11) winsock.exe injects file into (process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe. | | | |
| 2/5 | Injection | Writes into the memory of a process started from a created or modified executable | 1 | - |
| | • (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe modifies memory of (process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe. | | | |
| 2/5 | Injection | Modifies control flow of a process started from a created or modified executable | 1 | - |
| | • (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe alters context of (process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe. | | | |
| 2/5 | Task Scheduling | Schedules task | 3 | - |
| | • Schedules task for command "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe", to be triggered by Logon.<br>• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe", to be triggered by Logon.<br>• Schedules task for command "C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe", to be triggered by Time. Task has been rescheduled by the analyzer. | | | |
| 2/5 | Task Scheduling | Schedules task via schtasks | 2 | - |
| | • Schedules task "win defender run" via the schtasks command line utility.<br>• Schedules task "RtkAudioService64" via the schtasks command line utility. | | | |
| 1/5 | Mutex | Creates mutex | 4 | - |
| | • (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe creates mutex with name "runas".<br>• (Process #3) windef.exe creates mutex with name "QSR_MUTEX_0kBRNrRz5TDLEQoul0".<br>• (Process #11) winsock.exe creates mutex with name "QSR_MUTEX_0kBRNrRz5TDLEQoul0".<br>• (Process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe creates mutex with name "A743A547-9C1AFDB0-AEA27C97-73E39B07-D5BBC660F". | | | |
| 1/5 | Discovery | Enumerates running processes | 1 | - |
| | • (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe enumerates running processes. | | | |

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 1/5 | Hide Tracks | Creates process with hidden window | 7 | - |

- (Process #2) vnc.exe starts (process #4) svchost.exe with a hidden window.
- (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe starts (process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe with a hidden window.
- (Process #3) windef.exe starts (process #9) schtasks.exe with a hidden window.
- (Process #3) windef.exe starts (process #11) winsock.exe with a hidden window.
- (Process #11) winsock.exe starts (process #12) schtasks.exe with a hidden window.
- (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe starts (process #80) schtasks.exe with a hidden window.
- (Process #11) winsock.exe starts C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\pKg6lHYNIR2L.bat with a hidden window.

| | | | | |
|---|---|---|---|---|
| 1/5 | Obfuscation | Creates a page with write and execute permissions | 3 | - |

- (Process #2) vnc.exe changes the protection of a page in a foreign process from writable ("PAGE_READWRITE") to executable ("PAGE_EXECUTE_READ").
- (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.
- (Process #2) vnc.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.

| | | | | |
|---|---|---|---|---|
| 1/5 | Obfuscation | Reads from memory of another process | 1 | - |

- (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe reads from (process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe.

| | | | | |
|---|---|---|---|---|
| 1/5 | Persistence | Installs system startup script or application | 2 | - |

- (Process #3) windef.exe adds ""C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe"" to Windows startup via registry.
- (Process #11) winsock.exe adds ""C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe"" to Windows startup via registry.

| | | | | |
|---|---|---|---|---|
| 1/5 | Privilege Escalation | Enables process privilege | 1 | - |

- (Process #11) winsock.exe enables process privilege "SeDebugPrivilege".

| | | | | |
|---|---|---|---|---|
| 1/5 | Discovery | Reads system data | 1 | - |

- (Process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe reads the cryptographic machine GUID from registry.

| | | | | |
|---|---|---|---|---|
| 1/5 | Network Connection | Performs DNS request | 3 | - |

- (Process #3) windef.exe resolves host name "ip-api.com" to IP "208.95.112.1".
- (Process #11) winsock.exe resolves host name "sockartek.icu" to IP "-".
- (Process #11) winsock.exe resolves host name "ip-api.com" to IP "208.95.112.1".

| | | | | |
|---|---|---|---|---|
| 1/5 | Network Connection | Connects to remote host | 3 | - |

- (Process #3) windef.exe opens an outgoing TCP connection to host "208.95.112.1:80".
- (Process #11) winsock.exe opens an outgoing TCP connection to host "5.8.88.191:443".
- (Process #11) winsock.exe opens an outgoing TCP connection to host "208.95.112.1:80".

| | | | | |
|---|---|---|---|---|
| 1/5 | Network Connection | Tries to connect using an uncommon port | 1 | - |

- (Process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe tries to connect to TCP port 8000 at 50.17.5.224.

| | | | | |
|---|---|---|---|---|
| 1/5 | Execution | Drops PE file | 3 | - |

- (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe".
- (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe".
- (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe drops file "C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe".

| | | | | |
|---|---|---|---|---|
| 1/5 | Execution | Executes dropped PE file | 2 | - |

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| | • Executes dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe".<br>• Executes dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe". | | | |
| 1/5 | Execution | Executes itself | 1 | - |
| | • (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe. | | | |
| 1/5 | Obfuscation | Resolves API functions dynamically | 4 | - |
| | • (Process #1) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe resolves 55 API functions by name.<br>• (Process #3) windef.exe resolves 49 API functions by name.<br>• (Process #11) winsock.exe resolves 50 API functions by name.<br>• (Process #5) efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe resolves 77 API functions by name. | | | |

### Mitre ATT&CK Matrix

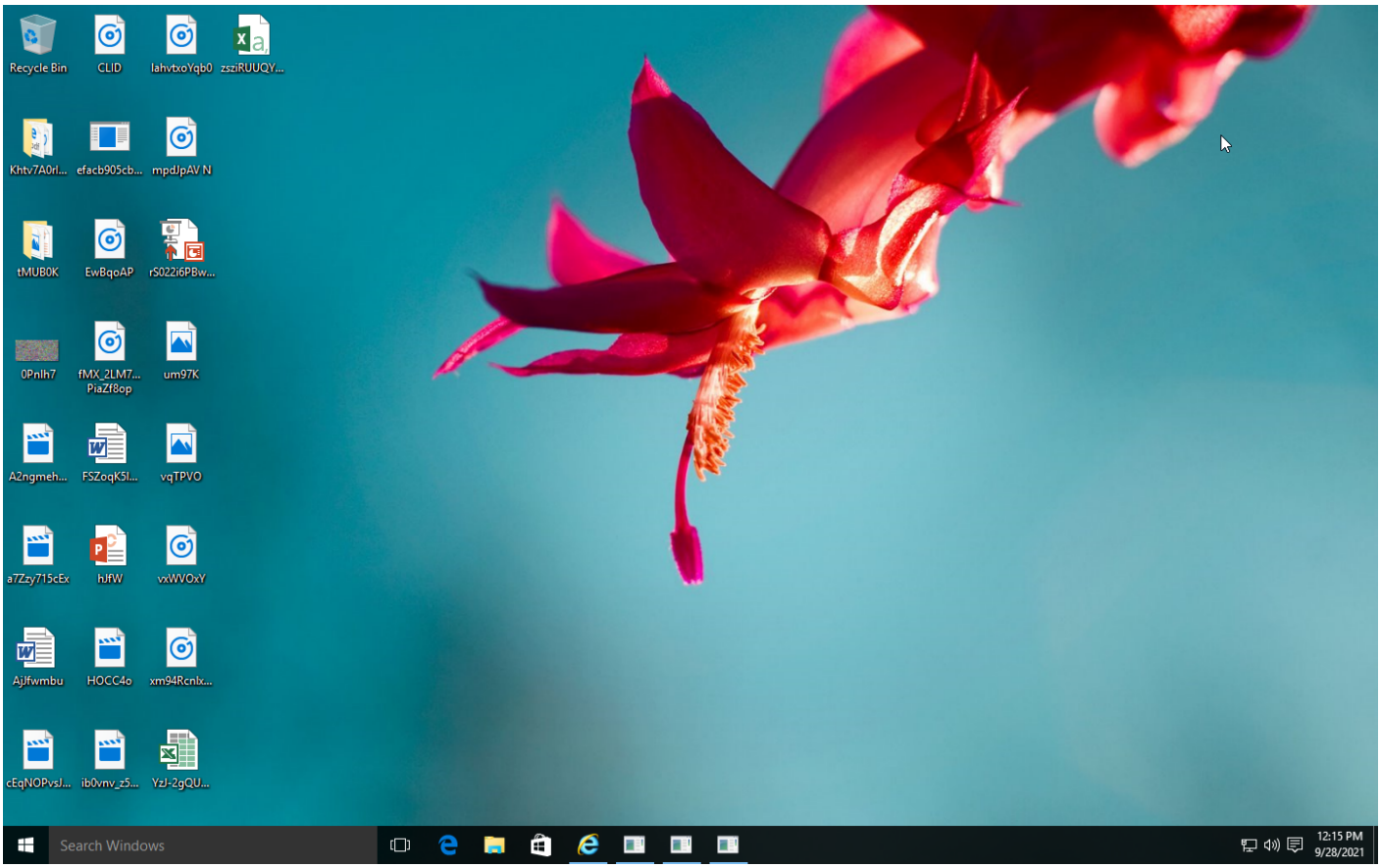
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | #T1047 Windows Management Instrumentation | #T1060 Registry Run Keys / Startup Folder | #T1179 Hooking | #T1143 Hidden Window | #T1056 Input Capture | #T1057 Process Discovery | | #T1056 Input Capture | #T1065 Uncommonly Used Port | | |
| | #T1053 Scheduled Task | #T1158 Hidden Files and Directories | #T1055 Process Injection | #T1045 Software Packing | #T1179 Hooking | #T1082 System Information Discovery | | | | | |
| | | #T1179 Hooking | #T1053 Scheduled Task | #T1096 NTFS File Attributes | | #T1016 System Network Configuration Discovery | | | | | |
| | | #T1053 Scheduled Task | | #T1112 Modify Registry | | #T1012 Query Registry | | | | | |
| | | | | #T1158 Hidden Files and Directories | | | | | | | |
| | | | | #T1055 Process Injection | | | | | | | |

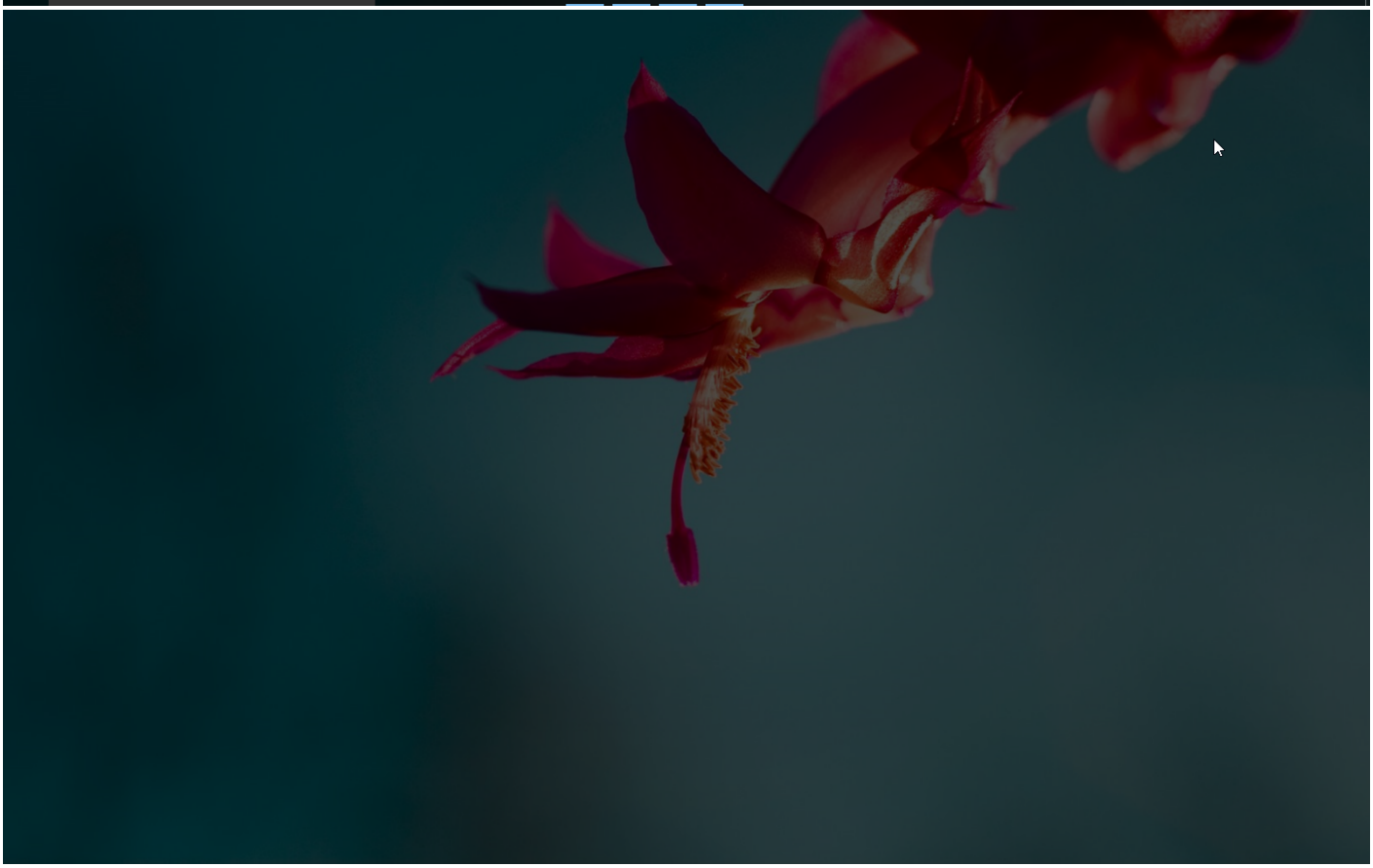
## Sample Information

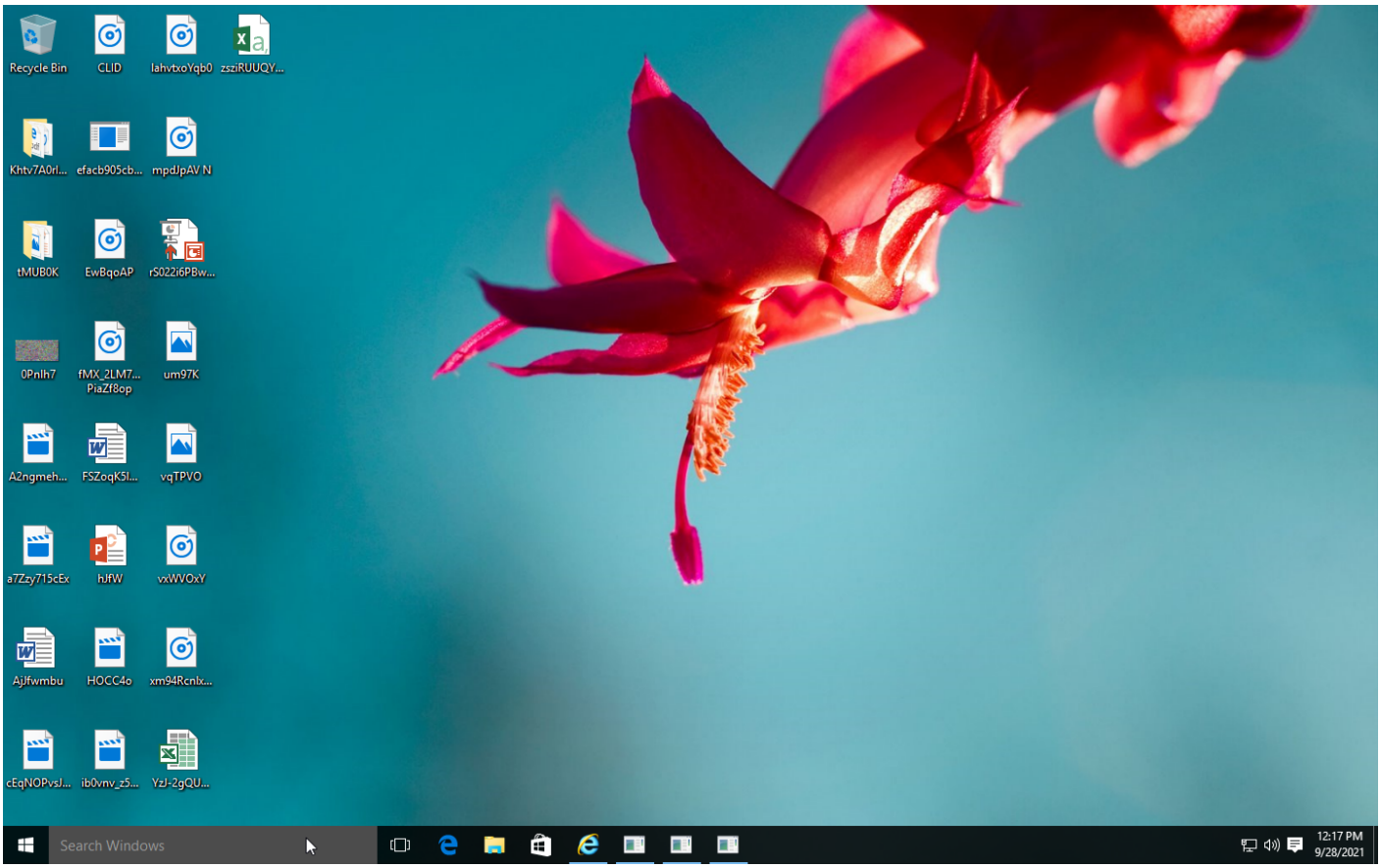
| | |
|---|---|
| ID | #2782920 |
| MD5 | b0b78da613422be0de8de2e2a2d0ce68 |
| SHA1 | a1aea30e16b3bbf15baf1fbb78499adcc5e11d97 |
| SHA256 | efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0 |
| SSDeep | 24576:su6J33O0c+JY5UZ+XC0kGso6Fal1lXgM6YmenKKSUlmDaGJTA4Pqa6jUvOkQwKYQ:2u0c++OCvkGs9Fap5aLKLkDl+dUvO9Yu |
| ImpHash | afcdf79be1557326c854b6e20cb900a7 |
| File Name | efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe |
| File Size | 2061.78 KB |
| Sample Type | Windows Exe (x86-32) |
| Has Macros | ✓ |

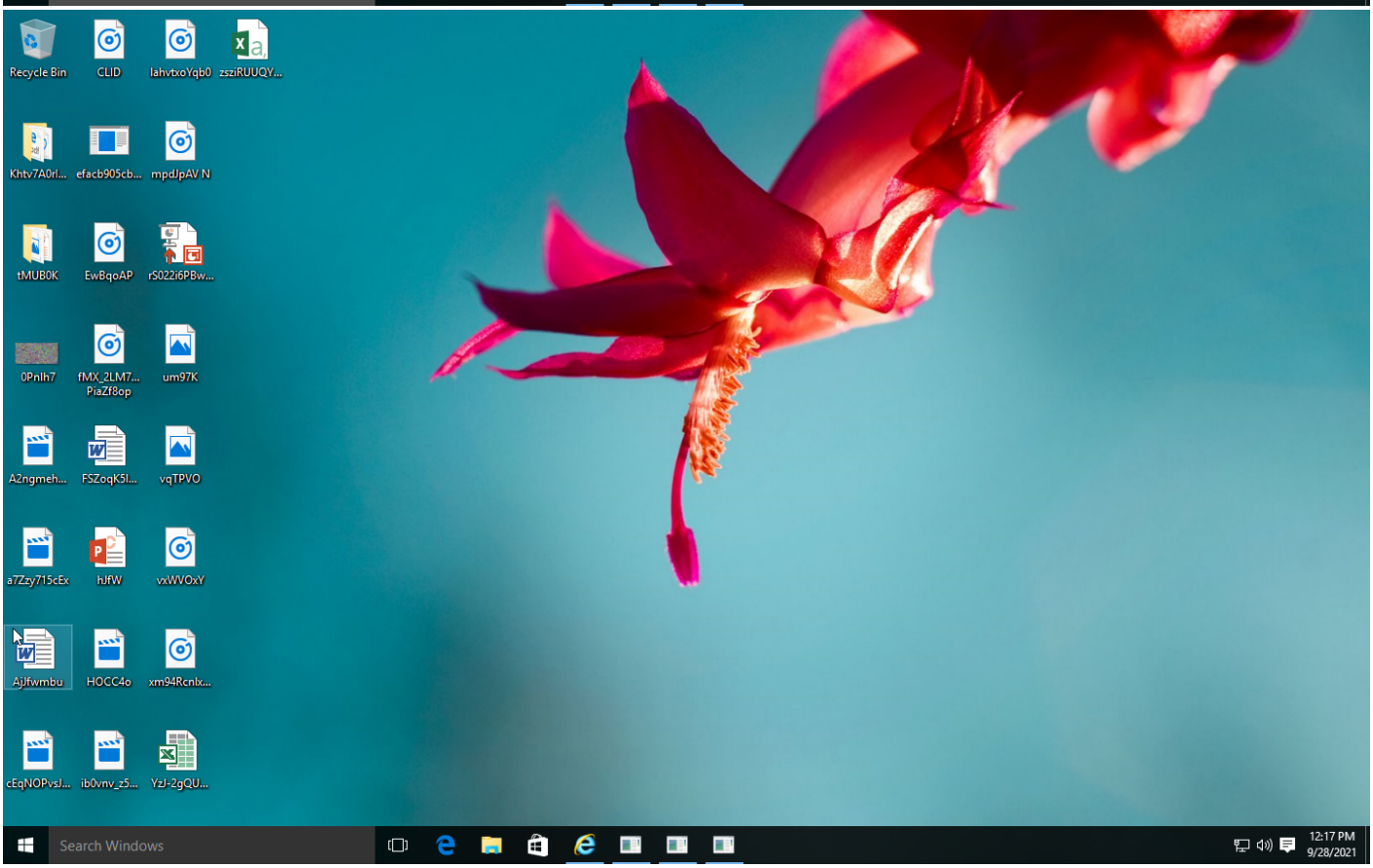
## Analysis Information

| | |
|---|---|
| Creation Time | 2021-09-28 14:14 (UTC+2) |
| Analysis Duration | 00:04:00 |
| Termination Reason | Timeout |
| Number of Monitored Processes | 80 |
| Execution Successful | False |
| Reputation Enabled | ✓ |
| WHOIS Enabled | ✓ |
| Built-in AV Enabled | ✓ |
| Built-in AV Applied On | Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files |
| Number of AV Matches | 34 |
| YARA Enabled | ✓ |
| YARA Applied On | Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files |
| Number of YARA Matches | 51 |


Recycle Bin
CLID
lahvtxoYqb0
zsziRUUQY...
Khtv7A0rl...
efacb905cb...
mpdJpAV N
tMUB0K
EwBqoAP
rS022i6PBw...
0Pnlh7
fMX_2LM7...
PiaZf8op
um97K
A2ngmeh...
FSZoqK5l...
vqTPVO
a7Zzy715cEx
hJfW
vxWVOxY
AjJfwmbu
HOCC4o
xm94Rcnlx...
cEqNOPvsJ...
ib0vnv_z5...
YzJ-2gQU...
Search Windows
12:15 PM
9/28/2021






Screenshots truncated

# NETWORK

## General

936 bytes total sent

1.09 KB total received

3 ports 80, 443, 8000

4 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

## DNS

3 DNS requests for 2 domains

1 nameservers contacted

1 total requests returned errors

## HTTP/S

2 URLs contacted, 2 servers

3 sessions, 936 bytes sent, 1.09 KB received

## HTTP Requests

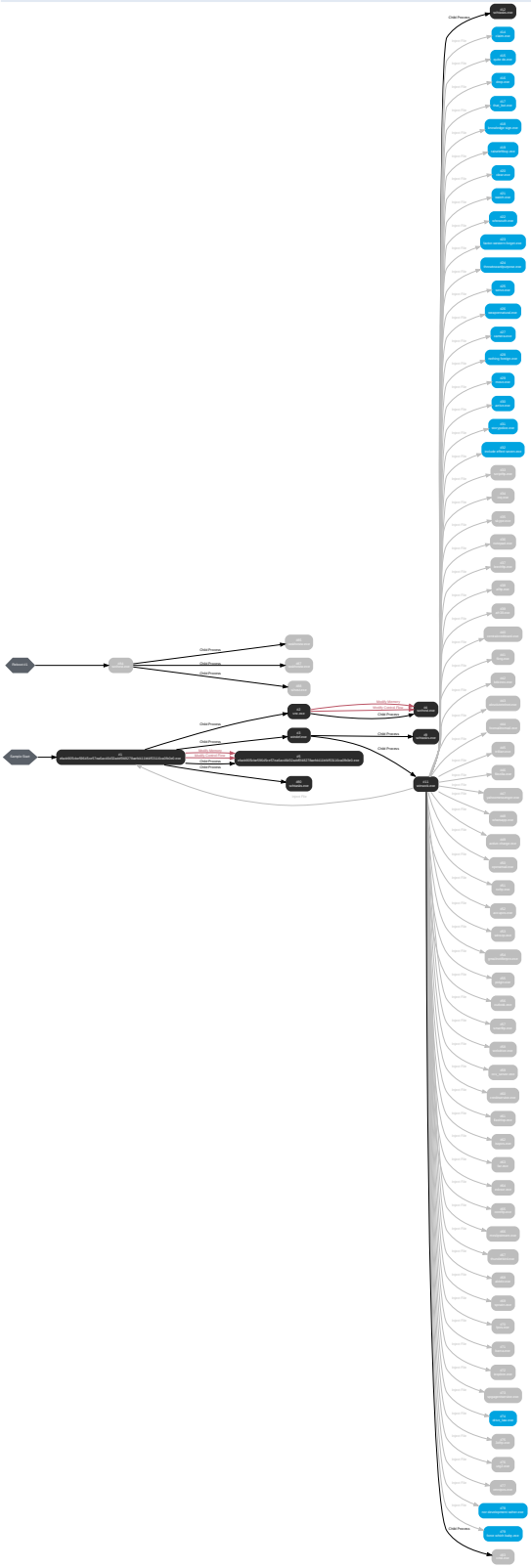
| Method | URL | Dest. IP | Dest. Port | Status Code | Response Size | Verdict |
|---|---|---|---|---|---|---|
| GET | http://ip-api.com/json/ | - | - | | 0 bytes | NA |
| POST | 0x21.in/_az/ | - | - | | 0 bytes | NA |

## DNS Requests

| Type | Hostname | Response Code | Resolved IPs | CNames | Verdict |
|---|---|---|---|---|---|
| A | ip-api.com | NoError | 208.95.112.1 | | NA |
| A | sockartek.icu | NXDomain | | | NA |

## BEHAVIOR

### Process Graph



### Process #1: efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe

| | |
|---|---|
| ID | 1 |
| File Name | c:\users\rdhj0cnfevzx\desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe |
| Command Line | "C:\Users\RDhJ0CNFevzX\Desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe" |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 80290, Reason: Analysis Target |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 240.07s |
| Return Code | Unknown |
| PID | 3200 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x74c | () | 0x57400 | ✗ | 1 |

### Dropped Files (3)

| File Name | File Size | SHA256 | YARA Match |
|---|---|---|---|
| C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe | 405.50 KB | 4e8a99cd33c9e5c747a3ce8f1a3e17824846f4a8f7cb0631aebd0815db2ce3a4 | ✗ |
| C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe | 349.00 KB | 7050608d53f80269df951d00883ed79815c060ce7678a76b5c3f6a2a985beea9 | ✗ |
| C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe | 2061.79 KB | 122e72d73d1b3a819fe2a9a7b06ca17ff20cd4f43346716de1794efa2318fdf7 | ✗ |

### Host Behavior

| Type | Count |
|---|---|
| Module | 106 |
| File | 59 |
| Environment | 2 |
| System | 2257 |
| Registry | 3 |
| - | 1 |
| Window | 2 |
| Mutex | 1 |
| Process | 237 |
| - | 3 |
| - | 11 |

### Process #2: vnc.exe

| | |
|---|---|
| ID | 2 |
| File Name | c:\users\rdhj0cnfevzx\appdata\local\temp\vnc.exe |
| Command Line | "C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe" |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 127568, Reason: Child Process |
| Unmonitor End Time | End Time: 161383, Reason: Terminated |
| Monitor duration | 33.81s |
| Return Code | 0 |
| PID | 2804 |
| Parent PID | 3200 |
| Bitness | 32 Bit |

### Host Behavior

| Type | Count |
|---|---|
| Module | 50 |
| System | 4 |
| Process | 2 |
| - | 8 |
| - | 10 |

### Process #3: windef.exe

| | |
|---|---|
| ID | 3 |
| File Name | c:\users\rdhj0cnfevzx\appdata\local\temp\windef.exe |
| Command Line | "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe" |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 129476, Reason: Child Process |
| Unmonitor End Time | End Time: 177538, Reason: Terminated |
| Monitor duration | 48.06s |
| Return Code | 0 |
| PID | 2080 |
| Parent PID | 3200 |
| Bitness | 32 Bit |

### Dropped Files (1)

| File Name | File Size | SHA256 | YARA Match |
|---|---|---|---|
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe | 349.00 KB | 7050608d53f80269df951d00883ed79815c060ce7678a76b5c3f6a2a985beea9 | ✗ |

### Host Behavior

| Type | Count |
|---|---|
| - | 12 |
| COM | 4 |
| Module | 56 |
| - | 1 |
| Mutex | 1 |
| Process | 2 |
| File | 28 |
| System | 3 |
| Registry | 24 |
| Environment | 4 |

### Network Behavior

| Type | Count |
|---|---|
| HTTP | 1 |
| DNS | 1 |
| TCP | 1 |

### Process #4: svchost.exe

| | |
|---|---|
| ID | 4 |
| File Name | c:\windows\system32\svchost.exe |
| Command Line | C:\Windows\system32\svchost.exe -k |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 129732, Reason: Child Process |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 190.63s |
| Return Code | Unknown |
| PID | 760 |
| Parent PID | 2804 |
| Bitness | 64 Bit |

### Injection Information (4)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Modify Memory | #2: c:\users\rdhj0cnfevzx\appdata\local\temp\vnc.exe | 0xbe4 | 0x680000(6815744) | 0x9c000 | ✓ | 1 |
| Modify Memory | #2: c:\users\rdhj0cnfevzx\appdata\local\temp\vnc.exe | 0xbe4 | 0x20000(131072) | 0x318 | ✓ | 1 |
| Modify Control Flow | #2: c:\users\rdhj0cnfevzx\appdata\local\temp\vnc.exe | 0xbe4 / 0xba0 | 0x25e000(2482176) | - | ✓ | 1 |
| Modify Memory | #2: c:\users\rdhj0cnfevzx\appdata\local\temp\vnc.exe | 0xbe4 | 0x7ff6bac63980(140697672235392) | 0x4 | ✓ | 1 |

### Host Behavior

| Type | Count |
|---|---|
| Module | 5 |

### Process #5: efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe

| | |
|---|---|
| ID | 5 |
| File Name | c:\users\rdhj0cnfevzx\desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe |
| Command Line | "C:\Users\RDhJ0CNFevzX\Desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe" |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 140531, Reason: Child Process |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 179.83s |
| Return Code | Unknown |
| PID | 4300 |
| Parent PID | 3200 |
| Bitness | 32 Bit |

### Injection Information (3)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Modify Memory | #1: c:\users\rdhj0cnfevzx\desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | 0x74c | 0xd0000(851968) | 0x20000 | ✓ | 1 |
| Modify Memory | #1: c:\users\rdhj0cnfevzx\desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | 0x74c | 0x3a0008(3801096) | 0x4 | ✓ | 1 |
| Modify Control Flow | #1: c:\users\rdhj0cnfevzx\desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | 0x74c / 0x910 | 0x77968fe0(2006355936) | - | ✓ | 1 |

### Host Behavior

| Type | Count |
|---|---|
| Module | 96 |
| Keyboard | 1 |
| System | 4 |
| Registry | 8 |
| User | 2 |
| Mutex | 1 |

### Network Behavior

| Type | Count |
|---|---|
| HTTP | 1 |
| TCP | 1 |

### Process #9: schtasks.exe

| | |
|---|---|
| ID | 9 |
| File Name | c:\windows\syswow64\schtasks.exe |
| Command Line | "schtasks" /create /tn "win defender run" /sc ONLOGON /tr "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe" /rl HIGHEST /f |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 171707, Reason: Child Process |
| Unmonitor End Time | End Time: 179267, Reason: Terminated |
| Monitor duration | 7.56s |
| Return Code | 0 |
| PID | 4184 |
| Parent PID | 2080 |
| Bitness | 32 Bit |

### Host Behavior

| Type | Count |
|---|---|
| Module | 3 |
| System | 3 |
| COM | 1 |
| File | 6 |

### Process #11: winsock.exe

| | |
|---|---|
| ID | 11 |
| File Name | c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe |
| Command Line | "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe" |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 173853, Reason: Child Process |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 146.50s |
| Return Code | Unknown |
| PID | 4276 |
| Parent PID | 2080 |
| Bitness | 32 Bit |

### Dropped Files (2)

| File Name | File Size | SHA256 | YARA Match |
|---|---|---|---|
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\Logs\09-28-2021 | 224 bytes | 6caf73d97aee0a7b4739383f336d9631e5095e28b16500e02860af64bdfca18b | ✗ |
| C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\pKg6lHYNIR2L.bat | 222 bytes | c0ea2f4aab400d15e49413011902be62a9f1dd0efdfeff250305204291a974ab | ✗ |

### Host Behavior

| Type | Count |
|---|---|
| - | 12 |
| COM | 4 |
| Module | 64 |
| - | 1 |
| Mutex | 1 |
| Process | 2 |
| File | 39 |
| System | 21 |
| Registry | 30 |
| Environment | 4 |
| User | 1 |
| Window | 6 |
| Keyboard | 5 |

### Network Behavior

| Type | Count |
|---|---|
| HTTP | 1 |
| DNS | 2 |
| TCP | 2 |

### Process #12: schtasks.exe

| | |
|---|---|
| ID | 12 |
| File Name | c:\windows\syswow64\schtasks.exe |
| Command Line | "schtasks" /create /tn "win defender run" /sc ONLOGON /tr "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe" /rl HIGHEST /f |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 188239, Reason: Child Process |
| Unmonitor End Time | End Time: 192982, Reason: Terminated |
| Monitor duration | 4.74s |
| Return Code | 0 |
| PID | 4696 |
| Parent PID | 4276 |
| Bitness | 32 Bit |

### Host Behavior

| Type | Count |
|---|---|
| Module | 3 |
| System | 3 |
| COM | 1 |
| File | 6 |

### Process #14: claim.exe

| | |
|---|---|
| ID | 14 |
| File Name | c:\program files\uninstall information\claim.exe |
| Command Line | "C:\Program Files\Uninstall Information\claim.exe" |
| Initial Working Directory | C:\Program Files\Uninstall Information\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 3380 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0xe6c | () | 0x57400 | ✗ | 1 |

### Process #15: quite do.exe

| | |
|---|---|
| ID | 15 |
| File Name | c:\program files\windows portable devices\quite do.exe |
| Command Line | "C:\Program Files\Windows Portable Devices\quite do.exe" |
| Initial Working Directory | C:\Program Files\Windows Portable Devices\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 3504 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0xd30 | () | 0x57400 | ✗ | 1 |

### Process #16: drop.exe

| | |
|---|---|
| ID | 16 |
| File Name | c:\program files\windows media player\drop.exe |
| Command Line | "C:\Program Files\Windows Media Player\drop.exe" |
| Initial Working Directory | C:\Program Files\Windows Media Player\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 3036 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0xda8 | () | 0x57400 | ✗ | 1 |

### Process #17: that_but.exe

| | |
|---|---|
| ID | 17 |
| File Name | c:\program files\windows defender\that_but.exe |
| Command Line | "C:\Program Files\Windows Defender\that_but.exe" |
| Initial Working Directory | C:\Program Files\Windows Defender\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 3220 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x394 | () | 0x57400 | ✗ | 1 |

### Process #18: knowledge sign.exe

| | |
|---|---|
| ID | 18 |
| File Name | c:\program files (x86)\windows multimedia platform\knowledge sign.exe |
| Command Line | "C:\Program Files (x86)\Windows Multimedia Platform\knowledge sign.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Multimedia Platform\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 2204 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0xb18 | () | 0x57400 | ✗ | 1 |

### Process #19: raiseleftbuy.exe

| | |
|---|---|
| ID | 19 |
| File Name | c:\program files (x86)\windowspowershell\raiseleftbuy.exe |
| Command Line | "C:\Program Files (x86)\WindowsPowerShell\raiseleftbuy.exe" |
| Initial Working Directory | C:\Program Files (x86)\WindowsPowerShell\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4136 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x102c | () | 0x57400 | ✗ | 1 |

### Process #20: clear.exe

| | |
|---|---|
| ID | 20 |
| File Name | c:\program files (x86)\windows photo viewer\clear.exe |
| Command Line | "C:\Program Files (x86)\Windows Photo Viewer\clear.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Photo Viewer\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4160 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1044 | () | 0x57400 | ✗ | 1 |

### Process #21: watch.exe

| | |
|---|---|
| ID | 21 |
| File Name | c:\program files\windows sidebar\watch.exe |
| Command Line | "C:\Program Files\Windows Sidebar\watch.exe" |
| Initial Working Directory | C:\Program Files\Windows Sidebar\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4116 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1018 | () | 0x57400 | ✗ | 1 |

### Process #22: whosouth.exe

| | |
|---|---|
| ID | 22 |
| File Name | c:\program files\internet explorer\whosouth.exe |
| Command Line | "C:\Program Files\Internet Explorer\whosouth.exe" |
| Initial Working Directory | C:\Program Files\Internet Explorer\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4152 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x103c | () | 0x57400 | ✗ | 1 |

### Process #23: factor-western-forget.exe

| | |
|---|---|
| ID | 23 |
| File Name | c:\program files (x86)\microsoft.net\factor-western-forget.exe |
| Command Line | "C:\Program Files (x86)\Microsoft.NET\factor-western-forget.exe" |
| Initial Working Directory | C:\Program Files (x86)\Microsoft.NET\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4176 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1054 | () | 0x57400 | ✗ | 1 |

### Process #24: throwtowardpurpose.exe

| | |
|---|---|
| ID | 24 |
| File Name | c:\program files\microsoft office 15\throwtowardpurpose.exe |
| Command Line | "C:\Program Files\Microsoft Office 15\throwtowardpurpose.exe" |
| Initial Working Directory | C:\Program Files\Microsoft Office 15\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4188 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1060 | () | 0x57400 | ✗ | 1 |

### Process #25: serve.exe

| | |
|---|---|
| ID | 25 |
| File Name | c:\program files\msbuild\serve.exe |
| Command Line | "C:\Program Files\MSBuild\serve.exe" |
| Initial Working Directory | C:\Program Files\MSBuild\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4252 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x10a0 | () | 0x57400 | ✗ | 1 |

### Process #26: weaponnatural.exe

| | |
|---|---|
| ID | 26 |
| File Name | c:\program files (x86)\windowspowershell\weaponnatural.exe |
| Command Line | "C:\Program Files (x86)\WindowsPowerShell\weaponnatural.exe" |
| Initial Working Directory | C:\Program Files (x86)\WindowsPowerShell\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4260 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x10a8 | () | 0x57400 | ✗ | 1 |

### Process #27: camera.exe

| | |
|---|---|
| ID | 27 |
| File Name | c:\program files\microsoft office 15\camera.exe |
| Command Line | "C:\Program Files\Microsoft Office 15\camera.exe" |
| Initial Working Directory | C:\Program Files\Microsoft Office 15\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4200 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x106c | () | 0x57400 | ✗ | 1 |

### Process #28: nothing foreign.exe

| | |
|---|---|
| ID | 28 |
| File Name | c:\program files\msbuild\nothing foreign.exe |
| Command Line | "C:\Program Files\MSBuild\nothing foreign.exe" |
| Initial Working Directory | C:\Program Files\MSBuild\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4224 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1084 | () | 0x57400 | ✗ | 1 |

### Process #29: move.exe

| | |
|---|---|
| ID | 29 |
| File Name | c:\program files (x86)\msbuild\move.exe |
| Command Line | "C:\Program Files (x86)\MSBuild\move.exe" |
| Initial Working Directory | C:\Program Files (x86)\MSBuild\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4232 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x108c | () | 0x57400 | ✗ | 1 |

### Process #30: arrive.exe

| | |
|---|---|
| ID | 30 |
| File Name | c:\program files (x86)\msbuild\arrive.exe |
| Command Line | "C:\Program Files (x86)\MSBuild\arrive.exe" |
| Initial Working Directory | C:\Program Files (x86)\MSBuild\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4208 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1074 | () | 0x57400 | ✗ | 1 |

### Process #31: storypolice.exe

| | |
|---|---|
| ID | 31 |
| File Name | c:\program files\windows multimedia platform\storypolice.exe |
| Command Line | "C:\Program Files\Windows Multimedia Platform\storypolice.exe" |
| Initial Working Directory | C:\Program Files\Windows Multimedia Platform\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4216 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x107c | () | 0x57400 | ✗ | 1 |

### Process #32: include effect seven.exe

| | |
|---|---|
| ID | 32 |
| File Name | c:\program files (x86)\windowspowershell\include effect seven.exe |
| Command Line | "C:\Program Files (x86)\WindowsPowerShell\include effect seven.exe" |
| Initial Working Directory | C:\Program Files (x86)\WindowsPowerShell\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4244 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1098 | () | 0x57400 | ✗ | 1 |

### Process #33: scriptftp.exe

| | |
|---|---|
| ID | 33 |
| File Name | c:\program files (x86)\microsoft.net\scriptftp.exe |
| Command Line | "C:\Program Files (x86)\Microsoft.NET\scriptftp.exe" |
| Initial Working Directory | C:\Program Files (x86)\Microsoft.NET\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4468 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1178 | () | 0x57400 | ✗ | 1 |

### Process #34: icq.exe

| | |
|---|---|
| ID | 34 |
| File Name | c:\program files\windowspowershell\icq.exe |
| Command Line | "C:\Program Files\WindowsPowerShell\icq.exe" |
| Initial Working Directory | C:\Program Files\WindowsPowerShell\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4500 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1198 | () | 0x57400 | ✗ | 1 |

### Process #35: skype.exe

| | |
|---|---|
| ID | 35 |
| File Name | c:\program files\windows nt\skype.exe |
| Command Line | "C:\Program Files\Windows NT\skype.exe" |
| Initial Working Directory | C:\Program Files\Windows NT\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4492 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1190 | () | 0x57400 | ✗ | 1 |

### Process #36: notepad.exe

| | |
|---|---|
| ID | 36 |
| File Name | c:\program files (x86)\reference assemblies\notepad.exe |
| Command Line | "C:\Program Files (x86)\Reference Assemblies\notepad.exe" |
| Initial Working Directory | C:\Program Files (x86)\Reference Assemblies\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4452 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1168 | () | 0x57400 | ✗ | 1 |

### Process #37: leechftp.exe

| | |
|---|---|
| ID | 37 |
| File Name | c:\program files (x86)\windows multimedia platform\leechftp.exe |
| Command Line | "C:\Program Files (x86)\Windows Multimedia Platform\leechftp.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Multimedia Platform\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4460 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1170 | () | 0x57400 | ✗ | 1 |

### Process #38: alftp.exe

| | |
|---|---|
| ID | 38 |
| File Name | c:\program files\windows multimedia platform\alftp.exe |
| Command Line | "C:\Program Files\Windows Multimedia Platform\alftp.exe" |
| Initial Working Directory | C:\Program Files\Windows Multimedia Platform\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4360 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x110c | () | 0x57400 | ✗ | 1 |

### Process #39: afr38.exe

| | |
|---|---|
| ID | 39 |
| File Name | c:\program files (x86)\windows portable devices\afr38.exe |
| Command Line | "C:\Program Files (x86)\Windows Portable Devices\afr38.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Portable Devices\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4612 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1208 | () | 0x57400 | ✗ | 1 |

### Process #40: centralcreditcard.exe

| | |
|---|---|
| ID | 40 |
| File Name | c:\program files\msbuild\centralcreditcard.exe |
| Command Line | "C:\Program Files\MSBuild\centralcreditcard.exe" |
| Initial Working Directory | C:\Program Files\MSBuild\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4792 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x12bc | () | 0x57400 | ✗ | 1 |

### Process #41: fling.exe

| | |
|---|---|
| ID | 41 |
| File Name | c:\program files\windows media player\fling.exe |
| Command Line | "C:\Program Files\Windows Media Player\fling.exe" |
| Initial Working Directory | C:\Program Files\Windows Media Player\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4396 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1130 | () | 0x57400 | ✗ | 1 |

### Process #42: bitkinex.exe

| | |
|---|---|
| ID | 42 |
| File Name | c:\program files (x86)\windows photo viewer\bitkinex.exe |
| Command Line | "C:\Program Files (x86)\Windows Photo Viewer\bitkinex.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Photo Viewer\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4428 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1150 | () | 0x57400 | ✗ | 1 |

### Process #43: absolutetelnet.exe

| | |
|---|---|
| ID | 43 |
| File Name | c:\program files (x86)\msbuild\absolutetelnet.exe |
| Command Line | "C:\Program Files (x86)\MSBuild\absolutetelnet.exe" |
| Initial Working Directory | C:\Program Files (x86)\MSBuild\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4376 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x111c | () | 0x57400 | ✗ | 1 |

### Process #44: foxmailincmail.exe

| | |
|---|---|
| ID | 44 |
| File Name | c:\program files\common files\foxmailincmail.exe |
| Command Line | "C:\Program Files\Common Files\foxmailincmail.exe" |
| Initial Working Directory | C:\Program Files\Common Files\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4524 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x11b0 | () | 0x57400 | ✗ | 1 |

### Process #45: trillian.exe

| | |
|---|---|
| ID | 45 |
| File Name | c:\program files (x86)\internet explorer\trillian.exe |
| Command Line | "C:\Program Files (x86)\Internet Explorer\trillian.exe" |
| Initial Working Directory | C:\Program Files (x86)\Internet Explorer\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4540 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x11c0 | () | 0x57400 | ✗ | 1 |

### Process #46: filezilla.exe

| | |
|---|---|
| ID | 46 |
| File Name | c:\program files\windows defender\filezilla.exe |
| Command Line | "C:\Program Files\Windows Defender\filezilla.exe" |
| Initial Working Directory | C:\Program Files\Windows Defender\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4412 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1140 | () | 0x57400 | ✗ | 1 |

### Process #47: yahoomessenger.exe

| | |
|---|---|
| ID | 47 |
| File Name | c:\program files (x86)\windows sidebar\yahoomessenger.exe |
| Command Line | "C:\Program Files (x86)\Windows Sidebar\yahoomessenger.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Sidebar\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4564 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x11d8 | () | 0x57400 | ✗ | 1 |

### Process #48: whatsapp.exe

| | |
|---|---|
| ID | 48 |
| File Name | c:\program files (x86)\msbuild\whatsapp.exe |
| Command Line | "C:\Program Files (x86)\MSBuild\whatsapp.exe" |
| Initial Working Directory | C:\Program Files (x86)\MSBuild\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4580 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x11e8 | () | 0x57400 | ✗ | 1 |

### Process #49: active-charge.exe

| | |
|---|---|
| ID | 49 |
| File Name | c:\program files (x86)\windows sidebar\active-charge.exe |
| Command Line | "C:\Program Files (x86)\Windows Sidebar\active-charge.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Sidebar\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4588 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x11f0 | () | 0x57400 | ✗ | 1 |

### Process #50: operamail.exe

| | |
|---|---|
| ID | 50 |
| File Name | c:\program files (x86)\microsoft.net\operamail.exe |
| Command Line | "C:\Program Files (x86)\Microsoft.NET\operamail.exe" |
| Initial Working Directory | C:\Program Files (x86)\Microsoft.NET\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4444 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1160 | () | 0x57400 | ✗ | 1 |

### Process #51: ncftp.exe

| | |
|---|---|
| ID | 51 |
| File Name | c:\program files\windows journal\ncftp.exe |
| Command Line | "C:\Program Files\Windows Journal\ncftp.exe" |
| Initial Working Directory | C:\Program Files\Windows Journal\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4484 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1188 | () | 0x57400 | ✗ | 1 |

### Process #52: accupos.exe

| | |
|---|---|
| ID | 52 |
| File Name | c:\program files (x86)\windows mail\accupos.exe |
| Command Line | "C:\Program Files (x86)\Windows Mail\accupos.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Mail\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4604 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1200 | () | 0x57400 | ✗ | 1 |

### Process #53: winscp.exe

| | |
|---|---|
| ID | 53 |
| File Name | c:\program files\windows mail\winscp.exe |
| Command Line | "C:\Program Files\Windows Mail\winscp.exe" |
| Initial Working Directory | C:\Program Files\Windows Mail\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4508 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x11a0 | () | 0x57400 | ✗ | 1 |

### Process #54: gmailnotifierpro.exe

| | |
|---|---|
| ID | 54 |
| File Name | c:\program files (x86)\windows photo viewer\gmailnotifierpro.exe |
| Command Line | "C:\Program Files (x86)\Windows Photo Viewer\gmailnotifierpro.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Photo Viewer\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4516 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x11a8 | () | 0x57400 | ✗ | 1 |

### Process #55: pidgin.exe

| | |
|---|---|
| ID | 55 |
| File Name | c:\program files\msbuild\pidgin.exe |
| Command Line | "C:\Program Files\MSBuild\pidgin.exe" |
| Initial Working Directory | C:\Program Files\MSBuild\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4476 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1180 | () | 0x57400 | ✗ | 1 |

### Process #56: outlook.exe

| | |
|---|---|
| ID | 56 |
| File Name | c:\program files (x86)\windows multimedia platform\outlook.exe |
| Command Line | "C:\Program Files (x86)\Windows Multimedia Platform\outlook.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Multimedia Platform\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4572 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x11e0 | () | 0x57400 | ✗ | 1 |

### Process #57: smartftp.exe

| | |
|---|---|
| ID | 57 |
| File Name | c:\program files\common files\smartftp.exe |
| Command Line | "C:\Program Files\Common Files\smartftp.exe" |
| Initial Working Directory | C:\Program Files\Common Files\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4556 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x11d0 | () | 0x57400 | ✗ | 1 |

### Process #58: webdrive.exe

| | |
|---|---|
| ID | 58 |
| File Name | c:\program files (x86)\windowspowershell\webdrive.exe |
| Command Line | "C:\Program Files (x86)\WindowsPowerShell\webdrive.exe" |
| Initial Working Directory | C:\Program Files (x86)\WindowsPowerShell\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4532 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x11b8 | () | 0x57400 | ✗ | 1 |

### Process #59: ccv_server.exe

| | |
|---|---|
| ID | 59 |
| File Name | c:\program files\reference assemblies\ccv_server.exe |
| Command Line | "C:\Program Files\Reference Assemblies\ccv_server.exe" |
| Initial Working Directory | C:\Program Files\Reference Assemblies\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4656 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1234 | () | 0x57400 | ✗ | 1 |

### Process #60: creditservice.exe

| | |
|---|---|
| ID | 60 |
| File Name | c:\program files (x86)\windows sidebar\creditservice.exe |
| Command Line | "C:\Program Files (x86)\Windows Sidebar\creditservice.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Sidebar\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4800 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x12c4 | () | 0x57400 | ✗ | 1 |

### Process #61: flashfxp.exe

| | |
|---|---|
| ID | 61 |
| File Name | c:\program files (x86)\reference assemblies\flashfxp.exe |
| Command Line | "C:\Program Files (x86)\Reference Assemblies\flashfxp.exe" |
| Initial Working Directory | C:\Program Files (x86)\Reference Assemblies\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4404 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1138 | () | 0x57400 | ✗ | 1 |

### Process #62: isspos.exe

| | |
|---|---|
| ID | 62 |
| File Name | c:\program files (x86)\windows sidebar\isspos.exe |
| Command Line | "C:\Program Files (x86)\Windows Sidebar\isspos.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Sidebar\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4852 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x12f8 | () | 0x57400 | ✗ | 1 |

### Process #63: far.exe

| | |
|---|---|
| ID | 63 |
| File Name | c:\program files\windows nt\far.exe |
| Command Line | "C:\Program Files\Windows NT\far.exe" |
| Initial Working Directory | C:\Program Files\Windows NT\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4420 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1148 | () | 0x57400 | ✗ | 1 |

### Process #64: edcsvr.exe

| | |
|---|---|
| ID | 64 |
| File Name | c:\program files (x86)\windows mail\edcsvr.exe |
| Command Line | "C:\Program Files (x86)\Windows Mail\edcsvr.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Mail\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4860 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1300 | () | 0x57400 | ✗ | 1 |

### Process #65: coreftp.exe

| | |
|---|---|
| ID | 65 |
| File Name | c:\program files (x86)\windows photo viewer\coreftp.exe |
| Command Line | "C:\Program Files (x86)\Windows Photo Viewer\coreftp.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Photo Viewer\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4436 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1158 | () | 0x57400 | ✗ | 1 |

### Process #66: mxslipstream.exe

| | |
|---|---|
| ID | 66 |
| File Name | c:\program files (x86)\windowspowershell\mxslipstream.exe |
| Command Line | "C:\Program Files (x86)\WindowsPowerShell\mxslipstream.exe" |
| Initial Working Directory | C:\Program Files (x86)\WindowsPowerShell\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4844 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x12f0 | () | 0x57400 | ✗ | 1 |

### Process #67: thunderbird.exe

| | |
|---|---|
| ID | 67 |
| File Name | c:\program files\common files\thunderbird.exe |
| Command Line | "C:\Program Files\Common Files\thunderbird.exe" |
| Initial Working Directory | C:\Program Files\Common Files\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4548 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x11c8 | () | 0x57400 | ✗ | 1 |

### Process #68: aldelo.exe

| | |
|---|---|
| ID | 68 |
| File Name | c:\program files (x86)\windows photo viewer\aldelo.exe |
| Command Line | "C:\Program Files (x86)\Windows Photo Viewer\aldelo.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Photo Viewer\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4624 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1214 | () | 0x57400 | ✗ | 1 |

### Process #69: spcwin.exe

| | |
|---|---|
| ID | 69 |
| File Name | c:\program files (x86)\internet explorer\spcwin.exe |
| Command Line | "C:\Program Files (x86)\Internet Explorer\spcwin.exe" |
| Initial Working Directory | C:\Program Files (x86)\Internet Explorer\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4896 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1324 | () | 0x57400 | ✗ | 1 |

### Process #70: fpos.exe

| | |
|---|---|
| ID | 70 |
| File Name | c:\program files (x86)\windows photo viewer\fpos.exe |
| Command Line | "C:\Program Files (x86)\Windows Photo Viewer\fpos.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows Photo Viewer\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4836 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x12e8 | () | 0x57400 | ✗ | 1 |

### Process #71: barca.exe

| | |
|---|---|
| ID | 71 |
| File Name | c:\program files\msbuild\barca.exe |
| Command Line | "C:\Program Files\MSBuild\barca.exe" |
| Initial Working Directory | C:\Program Files\MSBuild\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4388 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1128 | () | 0x57400 | ✗ | 1 |

### Process #72: iexplore.exe

| | |
|---|---|
| ID | 72 |
| File Name | c:\program files (x86)\internet explorer\iexplore.exe |
| Command Line | "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:572 CREDAT:82945 /prefetch:2 |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 3216 |
| Parent PID | 572 |
| Bitness | 32 Bit |

### Injection Information (2)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x13a4 | () | 0x57400 | ✗ | 1 |
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x4d8 | () | 0x57400 | ✗ | 1 |

### Process #73: spgagentservice.exe

| | |
|---|---|
| ID | 73 |
| File Name | c:\program files (x86)\internet explorer\spgagentservice.exe |
| Command Line | "C:\Program Files (x86)\Internet Explorer\spgagentservice.exe" |
| Initial Working Directory | C:\Program Files (x86)\Internet Explorer\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4908 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1330 | () | 0x57400 | ✗ | 1 |

### Process #74: drive_law.exe

| | |
|---|---|
| ID | 74 |
| File Name | c:\program files (x86)\internet explorer\drive_law.exe |
| Command Line | "C:\Program Files (x86)\Internet Explorer\drive_law.exe" |
| Initial Working Directory | C:\Program Files (x86)\Internet Explorer\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4976 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1374 | () | 0x57400 | ✗ | 1 |

### Process #75: 3dftp.exe

| | |
|---|---|
| ID | 75 |
| File Name | c:\program files\windows nt\3dftp.exe |
| Command Line | "C:\Program Files\Windows NT\3dftp.exe" |
| Initial Working Directory | C:\Program Files\Windows NT\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4368 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1114 | () | 0x57400 | ✗ | 1 |

### Process #76: utg2.exe

| | |
|---|---|
| ID | 76 |
| File Name | c:\program files\windows photo viewer\utg2.exe |
| Command Line | "C:\Program Files\Windows Photo Viewer\utg2.exe" |
| Initial Working Directory | C:\Program Files\Windows Photo Viewer\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4916 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1338 | () | 0x57400 | ✗ | 1 |

### Process #77: omnipos.exe

| | |
|---|---|
| ID | 77 |
| File Name | c:\program files\reference assemblies\omnipos.exe |
| Command Line | "C:\Program Files\Reference Assemblies\omnipos.exe" |
| Initial Working Directory | C:\Program Files\Reference Assemblies\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4868 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1308 | () | 0x57400 | ✗ | 1 |

### Process #78: nor development rather.exe

| | |
|---|---|
| ID | 78 |
| File Name | c:\program files (x86)\windows nt\nor development rather.exe |
| Command Line | "C:\Program Files (x86)\Windows NT\nor development rather.exe" |
| Initial Working Directory | C:\Program Files (x86)\Windows NT\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4984 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x137c | () | 0x57400 | ✗ | 1 |

### Process #79: force which baby.exe

| | |
|---|---|
| ID | 79 |
| File Name | c:\program files (x86)\windowspowershell\force which baby.exe |
| Command Line | "C:\Program Files (x86)\WindowsPowerShell\force which baby.exe" |
| Initial Working Directory | C:\Program Files (x86)\WindowsPowerShell\ |
| Monitor Start Time | Start Time: 190209, Reason: Injection |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 130.15s |
| Return Code | Unknown |
| PID | 4964 |
| Parent PID | 1600 |
| Bitness | 32 Bit |

### Injection Information (1)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Inject File | #11: c:\users\rdhj0cnfevzx\appdata\roaming\subdir\winsock.exe | 0x129c / 0x1368 | () | 0x57400 | ✗ | 1 |

### Process #80: schtasks.exe

| | |
|---|---|
| ID | 80 |
| File Name | c:\windows\syswow64\schtasks.exe |
| Command Line | "C:\Windows\SysWOW64\schtasks.exe" /create /tn RtkAudioService64 /tr "C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe" /sc minute /mo 1 /F |
| Initial Working Directory | C:\Windows\SysWOW64\ |
| Monitor Start Time | Start Time: 205448, Reason: Child Process |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 114.91s |
| Return Code | Unknown |
| PID | 4880 |
| Parent PID | 3200 |
| Bitness | 32 Bit |

### Host Behavior

| Type | Count |
|---|---|
| Module | 3 |
| System | 3 |
| COM | 1 |

### Process #83: cmd.exe

| | |
|---|---|
| ID | 83 |
| File Name | c:\windows\syswow64\cmd.exe |
| Command Line | C:\Windows\system32\cmd.exe /c ""C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\pKg6lHYNlR2L.bat" " |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 220915, Reason: Child Process |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 99.44s |
| Return Code | Unknown |
| PID | 3324 |
| Parent PID | 4276 |
| Bitness | 32 Bit |

### Process #84: svchost.exe

| | |
|---|---|
| ID | 84 |
| File Name | c:\windows\system32\svchost.exe |
| Command Line | C:\Windows\system32\svchost.exe -k netsvcs |
| Initial Working Directory | C:\Windows\system32\ |
| Monitor Start Time | Start Time: 245902, Reason: Created Scheduled Job |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 74.46s |
| Return Code | Unknown |
| PID | 1000 |
| Parent PID | 532 |
| Bitness | 64 Bit |

### Process #85: taskhostw.exe

| | |
|---|---|
| ID | 85 |
| File Name | c:\windows\system32\taskhostw.exe |
| Command Line | taskhostw.exe SYSTEM |
| Initial Working Directory | C:\Windows\system32\ |
| Monitor Start Time | Start Time: 279569, Reason: Child Process |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 40.79s |
| Return Code | Unknown |
| PID | 1224 |
| Parent PID | 1000 |
| Bitness | 64 Bit |

### Process #87: taskhostw.exe

| | |
|---|---|
| ID | 87 |
| File Name | c:\windows\system32\taskhostw.exe |
| Command Line | taskhostw.exe |
| Initial Working Directory | C:\Windows\system32\ |
| Monitor Start Time | Start Time: 290067, Reason: Child Process |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 30.29s |
| Return Code | Unknown |
| PID | 1460 |
| Parent PID | 1000 |
| Bitness | 64 Bit |

### Process #88: sihost.exe

| | |
|---|---|
| ID | 88 |
| File Name | c:\windows\system32\sihost.exe |
| Command Line | sihost.exe |
| Initial Working Directory | C:\Windows\system32\ |
| Monitor Start Time | Start Time: 290084, Reason: Child Process |
| Unmonitor End Time | End Time: 320358, Reason: Terminated by Timeout |
| Monitor duration | 30.27s |
| Return Code | Unknown |
| PID | 1468 |
| Parent PID | 1000 |
| Bitness | 64 Bit |

# ARTIFACTS

## File

| SHA256 | File Names | Category | File Size | MIME Type | Operations | Verdict |
|---|---|---|---|---|---|---|
| efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0 | C:\Users\RDhJ0CNFevzX\Desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | Sample File | 2061.78 KB | application/vnd.microsoft.portable-executable | Access, Read | MALICIOUS |
| 122e72d73d1b3a819fe2a9a7b06ca17ff20cd4f43346716de1794efa2318fdf7 | SystemPropertiesPerformance.exe, C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe | Dropped File | 2061.79 KB | application/vnd.microsoft.portable-executable | Access, Write, Create | MALICIOUS |
| 4e8a99cd33c9e5c747a3ce8f1a3e17824846f4a8f7cb0631aebd0815db2ce3a4 | C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe | Dropped File | 405.50 KB | application/vnd.microsoft.portable-executable | Access, Write, Create | MALICIOUS |
| 7050608d53f80269df951d00883ed79815c060ce7678a76b5c3f6a2a985beea9 | C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\windef.exe | Dropped File | 349.00 KB | application/vnd.microsoft.portable-executable | Access, Write, Create | MALICIOUS |
| c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858 | c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat | Modified File | 128 bytes | application/octet-stream | - | CLEAN |
| 6caf73d97aee0a7b4739383f336d9631e5095e28b16500e02860af64bdfca18b | C:\Users\RDhJ0CNFevzX\AppData\Roaming\Logs\09-28-2021 | Dropped File | 224 bytes | application/octet-stream | Access, Write, Create | CLEAN |
| c0ea2f4aab400d15e49413011902be62a9f1dd0efdfeff250305204291a974ab | C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\pKg6lHYNIR2L.bat | Dropped File | 222 bytes | text/x-msdos-batch | Access, Write, Create | CLEAN |

## Filename

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe | Dropped File | Access, Write, Create | SUSPICIOUS |
| C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe | Dropped File | Access, Write, Create | SUSPICIOUS |
| C:\Users\RDhJ0CNFevzX\Desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | Sample File | Access, Read | CLEAN |
| C:\Users\RDhJ0CNFevzX\Desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe:Zone.Identifier | Accessed File | Access | CLEAN |
| C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe | Dropped File | Access, Write, Create | CLEAN |
| C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe | Dropped File | Access, Write, Create | CLEAN |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | Accessed File | Access, Read | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\windef.exe.config | Accessed File | Access | CLEAN |
| C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe:Zone.Identifier | Accessed File | Access, Delete | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir | Accessed File | Access, Create | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\windef.exe | Dropped File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe:Zone.Identifier | Accessed File | Access, Delete | CLEAN |
| C:\Windows\SysWOW64\schtasks.exe | Accessed File | Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe.config | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\Logs | Accessed File | Access, Create | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\Logs\09-28-2021 | Dropped File | Access, Write, Create | CLEAN |
| C:\Users\RDhJ0CNFevzX\btpanui | Accessed File | Access, Create | CLEAN |
| SystemPropertiesPerformance.exe | Dropped File | Access | CLEAN |
| btpanui | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\pKg6lHYNlR2L.bat | Dropped File | Access, Write, Create | CLEAN |

## URL

| URL | Category | IP Address | Country | HTTP Methods | Verdict |
|---|---|---|---|---|---|
| http://ip-api.com/json/ | - | 208.95.112.1 | - | GET | CLEAN |
| http://0x21.in/_az/ | - | 50.17.5.224 | - | POST | CLEAN |

## Domain

| Domain | IP Address | Country | Protocols | Verdict |
|---|---|---|---|---|
| ip-api.com | 208.95.112.1 | - | HTTP, DNS | CLEAN |
| 0x21.in | 50.17.5.224 | - | HTTP | CLEAN |
| sockartek.icu | - | - | DNS | CLEAN |

## IP

| IP Address | Domains | Country | Protocols | Verdict |
|---|---|---|---|---|
| 192.168.0.1 | - | - | UDP, DNS | CLEAN |
| 208.95.112.1 | ip-api.com | United States | HTTP, DNS, TCP | CLEAN |
| 5.8.88.191 | - | Russia | TCP | CLEAN |
| 50.17.5.224 | 0x21.in | United States | HTTP, DNS, TCP | CLEAN |

## Mutex

| Name | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| runas | access | efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | CLEAN |
| QSR_MUTEX_0kBRNrRz5TDLEQoul0 | access | windef.exe | CLEAN |
| A743A547-9C1AFDB0-AEA27C97-73E39B07-D5BBC660F | access | efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | CLEAN |

## Registry

| Registry Key | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| HKEY_CURRENT_USER\Control Panel\Mouse | access | efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | CLEAN |
| HKEY_CURRENT_USER\Control Panel\Mouse\SwapMouseButtons | access, read | efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | CLEAN |
| HKEY_CURRENT_USER\Software\AutoIt v3\AutoIt | access | efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion | access | windef.exe, winsock.exe | CLEAN |

| Registry Key | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType | access, read | windef.exe, winsock.exe | CLEAN |
| HKEY_CURRENT_USER | access | windef.exe, winsock.exe | CLEAN |
| HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections | access | windef.exe, winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections | access | windef.exe, winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings | access | windef.exe, winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework | access | windef.exe, winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport | access, read | windef.exe, winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time | access | windef.exe, winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI | access, read | windef.exe, winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST | access | windef.exe, winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display | access, read | windef.exe, winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std | access, read | windef.exe, winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt | access, read | windef.exe, winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 | access | windef.exe, winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind | access, read | windef.exe, winsock.exe | CLEAN |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run | access | windef.exe, winsock.exe | CLEAN |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\win defender run | access, read, write | windef.exe, winsock.exe | CLEAN |
| HKEY_PERFORMANCE_DATA | access | windef.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework | access | winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting | access, read | winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger | access, read | winsock.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography | access | efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid | access, read | efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion | access, create | efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName | access, read | efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | CLEAN |

## Process

| Process Name | Commandline | Verdict |
|---|---|---|
| vnc.exe | "C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe" | MALICIOUS |
| windef.exe | "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe" | MALICIOUS |
| winsock.exe | "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe" | MALICIOUS |

| Process Name | Commandline | Verdict |
|---|---|---|
| efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | "C:\Users\RDhJ0CNFevzX\Desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe" | SUSPICIOUS |
| svchost.exe | C:\Windows\system32\svchost.exe -k | SUSPICIOUS |
| efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | "C:\Users\RDhJ0CNFevzX\Desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe" | SUSPICIOUS |
| schtasks.exe | "schtasks" /create /tn "win defender run" /sc ONLOGON /tr "C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe" /rl HIGHEST /f | SUSPICIOUS |
| schtasks.exe | "schtasks" /create /tn "win defender run" /sc ONLOGON /tr "C:\Users\RDhJ0CNFevzX\AppData\Roaming\SubDir\winsock.exe" /rl HIGHEST /f | SUSPICIOUS |
| schtasks.exe | "C:\Windows\SysWOW64\schtasks.exe" /create /tn RtkAudioService64 /tr "C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe" /sc minute /mo 1 /F | SUSPICIOUS |
| claim.exe | "C:\Program Files\Uninstall Information\claim.exe" | CLEAN |
| quite do.exe | "C:\Program Files\Windows Portable Devices\quite do.exe" | CLEAN |
| drop.exe | "C:\Program Files\Windows Media Player\drop.exe" | CLEAN |
| that_but.exe | "C:\Program Files\Windows Defender\that_but.exe" | CLEAN |
| knowledge sign.exe | "C:\Program Files (x86)\Windows Multimedia Platform\knowledge sign.exe" | CLEAN |
| raiseleftbuy.exe | "C:\Program Files (x86)\WindowsPowerShell\raiseleftbuy.exe" | CLEAN |
| clear.exe | "C:\Program Files (x86)\Windows Photo Viewer\clear.exe" | CLEAN |
| watch.exe | "C:\Program Files\Windows Sidebar\watch.exe" | CLEAN |
| whosouth.exe | "C:\Program Files\Internet Explorer\whosouth.exe" | CLEAN |
| factor-western-forget.exe | "C:\Program Files (x86)\Microsoft.NET\factor-western-forget.exe" | CLEAN |
| throwtowardpurpose.exe | "C:\Program Files\Microsoft Office 15\throwtowardpurpose.exe" | CLEAN |
| serve.exe | "C:\Program Files\MSBuild\serve.exe" | CLEAN |
| weaponnatural.exe | "C:\Program Files (x86)\WindowsPowerShell\weaponnatural.exe" | CLEAN |
| camera.exe | "C:\Program Files\Microsoft Office 15\camera.exe" | CLEAN |
| nothing foreign.exe | "C:\Program Files\MSBuild\nothing foreign.exe" | CLEAN |
| move.exe | "C:\Program Files (x86)\MSBuild\move.exe" | CLEAN |
| arrive.exe | "C:\Program Files (x86)\MSBuild\arrive.exe" | CLEAN |
| storypolice.exe | "C:\Program Files\Windows Multimedia Platform\storypolice.exe" | CLEAN |
| include effect seven.exe | "C:\Program Files (x86)\WindowsPowerShell\include effect seven.exe" | CLEAN |
| scriptftp.exe | "C:\Program Files (x86)\Microsoft.NET\scriptftp.exe" | CLEAN |
| icq.exe | "C:\Program Files\WindowsPowerShell\icq.exe" | CLEAN |
| skype.exe | "C:\Program Files\Windows NT\skype.exe" | CLEAN |
| notepad.exe | "C:\Program Files (x86)\Reference Assemblies\notepad.exe" | CLEAN |
| leechftp.exe | "C:\Program Files (x86)\Windows Multimedia Platform\leechftp.exe" | CLEAN |
| alftp.exe | "C:\Program Files\Windows Multimedia Platform\alftp.exe" | CLEAN |
| afr38.exe | "C:\Program Files (x86)\Windows Portable Devices\afr38.exe" | CLEAN |
| centralcreditcard.exe | "C:\Program Files\MSBuild\centralcreditcard.exe" | CLEAN |
| fling.exe | "C:\Program Files\Windows Media Player\fling.exe" | CLEAN |

| Process Name | Commandline | Verdict |
|---|---|---|
| bitkinex.exe | "C:\Program Files (x86)\Windows Photo Viewer\bitkinex.exe" | CLEAN |
| absolutetelnet.exe | "C:\Program Files (x86)\MSBuild\absolutetelnet.exe" | CLEAN |
| foxmailincmail.exe | "C:\Program Files\Common Files\foxmailincmail.exe" | CLEAN |
| trillian.exe | "C:\Program Files (x86)\Internet Explorer\trillian.exe" | CLEAN |
| filezilla.exe | "C:\Program Files\Windows Defender\filezilla.exe" | CLEAN |
| yahoomessenger.exe | "C:\Program Files (x86)\Windows Sidebar\yahoomessenger.exe" | CLEAN |
| whatsapp.exe | "C:\Program Files (x86)\MSBuild\whatsapp.exe" | CLEAN |
| active-charge.exe | "C:\Program Files (x86)\Windows Sidebar\active-charge.exe" | CLEAN |
| operamail.exe | "C:\Program Files (x86)\Microsoft.NET\operamail.exe" | CLEAN |
| ncftp.exe | "C:\Program Files\Windows Journal\ncftp.exe" | CLEAN |
| accupos.exe | "C:\Program Files (x86)\Windows Mail\accupos.exe" | CLEAN |
| winscp.exe | "C:\Program Files\Windows Mail\winscp.exe" | CLEAN |
| gmailnotifierpro.exe | "C:\Program Files (x86)\Windows Photo Viewer\gmailnotifierpro.exe" | CLEAN |
| pidgin.exe | "C:\Program Files\MSBuild\pidgin.exe" | CLEAN |
| outlook.exe | "C:\Program Files (x86)\Windows Multimedia Platform\outlook.exe" | CLEAN |
| smartftp.exe | "C:\Program Files\Common Files\smartftp.exe" | CLEAN |
| webdrive.exe | "C:\Program Files (x86)\WindowsPowerShell\webdrive.exe" | CLEAN |
| ccv_server.exe | "C:\Program Files\Reference Assemblies\ccv_server.exe" | CLEAN |
| creditservice.exe | "C:\Program Files (x86)\Windows Sidebar\creditservice.exe" | CLEAN |
| flashfxp.exe | "C:\Program Files (x86)\Reference Assemblies\flashfxp.exe" | CLEAN |
| isspos.exe | "C:\Program Files (x86)\Windows Sidebar\isspos.exe" | CLEAN |
| far.exe | "C:\Program Files\Windows NT\far.exe" | CLEAN |
| edcsvr.exe | "C:\Program Files (x86)\Windows Mail\edcsvr.exe" | CLEAN |
| coreftp.exe | "C:\Program Files (x86)\Windows Photo Viewer\coreftp.exe" | CLEAN |
| mxslipstream.exe | "C:\Program Files (x86)\WindowsPowerShell\mxslipstream.exe" | CLEAN |
| thunderbird.exe | "C:\Program Files\Common Files\thunderbird.exe" | CLEAN |
| aldelo.exe | "C:\Program Files (x86)\Windows Photo Viewer\aldelo.exe" | CLEAN |
| spcwin.exe | "C:\Program Files (x86)\Internet Explorer\spcwin.exe" | CLEAN |
| fpos.exe | "C:\Program Files (x86)\Windows Photo Viewer\fpos.exe" | CLEAN |
| barca.exe | "C:\Program Files\MSBuild\barca.exe" | CLEAN |
| iexplore.exe | "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:572 CREDAT:82945 /prefetch:2 | CLEAN |
| spgagentservice.exe | "C:\Program Files (x86)\Internet Explorer\spgagentservice.exe" | CLEAN |
| drive_law.exe | "C:\Program Files (x86)\Internet Explorer\drive_law.exe" | CLEAN |
| 3dftp.exe | "C:\Program Files\Windows NT\3dftp.exe" | CLEAN |
| utg2.exe | "C:\Program Files\Windows Photo Viewer\utg2.exe" | CLEAN |
| omnipos.exe | "C:\Program Files\Reference Assemblies\omnipos.exe" | CLEAN |

| Process Name | Commandline | Verdict |
|---|---|---|
| nor development rather.exe | "C:\Program Files (x86)\Windows NT\nor development rather.exe" | CLEAN |
| force which baby.exe | "C:\Program Files (x86)\WindowsPowerShell\force which baby.exe" | CLEAN |
| cmd.exe | C:\Windows\system32\cmd.exe /c ""C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\pKg6lHYNlR2L.bat" " | CLEAN |
| taskhostw.exe | taskhostw.exe SYSTEM | CLEAN |
| taskhostw.exe | taskhostw.exe | CLEAN |
| sihost.exe | sihost.exe | CLEAN |

## YARA / AV

### YARA (51)

| Ruleset Name | Rule Name | Rule Description | File Type | File Name | Classification | Verdict |
|---|---|---|---|---|---|---|
| RATs | QuasarRATCommands_1_3 | Quasar RAT ver 1.3 packets | Dropped File | C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe | Backdoor, Spyware | 5/5 |
| RATs | Quasar_RAT_2 | Quasar RAT | Dropped File | C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe | Backdoor, Spyware | 5/5 |
| RATs | xRAT_1 | xRAT malware | Dropped File | C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe | Backdoor | 5/5 |
| RATs | xrat_quasarrat | xRAT malware | Dropped File | C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe | Backdoor | 5/5 |
| RATs | QuasarRATCommands_1_3 | Quasar RAT ver 1.3 packets | Sample File | C:\Users\RDhJ0CNFevzX\Desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | Backdoor, Spyware | 5/5 |
| RATs | Quasar_RAT_2 | Quasar RAT | Sample File | C:\Users\RDhJ0CNFevzX\Desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | Backdoor, Spyware | 5/5 |
| RATs | xrat_quasarrat | xRAT malware | Sample File | C:\Users\RDhJ0CNFevzX\Desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | Backdoor | 5/5 |
| RATs | QuasarRATCommands_1_3 | Quasar RAT ver 1.3 packets | Dropped File | C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe | Backdoor, Spyware | 5/5 |
| RATs | Quasar_RAT_2 | Quasar RAT | Dropped File | C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe | Backdoor, Spyware | 5/5 |
| RATs | xrat_quasarrat | xRAT malware | Dropped File | C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe | Backdoor | 5/5 |
| RATs | QuasarRATCommands_1_3 | Quasar RAT ver 1.3 packets | Dropped File | C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe | Backdoor, Spyware | 5/5 |
| RATs | Quasar_RAT_2 | Quasar RAT | Dropped File | C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe | Backdoor, Spyware | 5/5 |
| RATs | xRAT_1 | xRAT malware | Dropped File | C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe | Backdoor | 5/5 |
| RATs | xrat_quasarrat | xRAT malware | Dropped File | C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe | Backdoor | 5/5 |
| RATs | QuasarRATCommands_1_3 | Quasar RAT ver 1.3 packets | Memory Dump | - | Backdoor, Spyware | 5/5 |
| RATs | Quasar_RAT_2 | Quasar RAT | Memory Dump | - | Backdoor, Spyware | 5/5 |
| RATs | xrat_quasarrat | xRAT malware | Memory Dump | - | Backdoor | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| RATs | QuasarRATCommands_1_3 | Quasar RAT ver 1.3 packets | Memory Dump | - | Backdoor, Spyware | 5/5 |
| RATs | Quasar_RAT_2 | Quasar RAT | Memory Dump | - | Backdoor, Spyware | 5/5 |
| RATs | xrat_quasarrat | xRAT malware | Memory Dump | - | Backdoor | 5/5 |
| RATs | QuasarRATCommands_1_3 | Quasar RAT ver 1.3 packets | Memory Dump | - | Backdoor, Spyware | 5/5 |

| Ruleset Name | Rule Name | Rule Description | File Type | File Name | Classification | Verdict |
|---|---|---|---|---|---|---|
| RATs | Quasar_RAT_2 | Quasar RAT | Memory Dump | - | Backdoor, Spyware | 5/5 |
| RATs | xRAT_1 | xRAT malware | Memory Dump | - | Backdoor | 5/5 |
| RATs | xrat_quasarrat | xRAT malware | Memory Dump | - | Backdoor | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| RATs | QuasarRATCommands_1_3 | Quasar RAT ver 1.3 packets | Memory Dump | - | Backdoor, Spyware | 5/5 |
| RATs | Quasar_RAT_2 | Quasar RAT | Memory Dump | - | Backdoor, Spyware | 5/5 |
| RATs | xrat_quasarrat | xRAT malware | Memory Dump | - | Backdoor | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |
| Malware | Azorult_Generic | Azorult v2 and v3 | Memory Dump | - | Spyware | 5/5 |

### Antivirus (34)

| File Type | Threat Name | File Name | Verdict |
|---|---|---|---|
| Sample File | Trojan.GenericKD.41182905 | C:\Users\RDhJ0CNFevzX\Desktop\efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0.exe | MALICIOUS |
| Dropped File | Trojan.GenericKD.44524794 | C:\Users\RDHJ0C~1\AppData\Local\Temp\vnc.exe | MALICIOUS |
| Dropped File | Trojan.GenericKD.43426068 | C:\Users\RDHJ0C~1\AppData\Local\Temp\windef.exe | MALICIOUS |

| File Type | Threat Name | File Name | Verdict |
|---|---|---|---|
| Dropped File | Trojan.GenericKD.41182905 | C:\Users\RDhJ0CNFevzX\btpanui\SystemPropertiesPerformance.exe | MALICIOUS |
| Memory Dump | Gen:Variant.Fugrafa.7193 | - | MALICIOUS |
| Memory Dump | Gen:Variant.Graftor.774294 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Gen:Variant.Fugrafa.7193 | - | MALICIOUS |
| Memory Dump | Gen:Variant.Razy.681395 | - | MALICIOUS |
| Memory Dump | Gen:Variant.Graftor.774294 | - | MALICIOUS |
| Memory Dump | Trojan.PWS.ZNN | - | MALICIOUS |
| Memory Dump | Gen:Variant.Fugrafa.7193 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |
| Memory Dump | Generic.Delph.PWS.D0207221 | - | MALICIOUS |

# ENVIRONMENT

### Virtual Machine Information

| | |
|---|---|
| Name | win10_64_th2_en_mso2016 |
| Description | win10_64_th2_en_mso2016 |
| Architecture | x86 64-bit |
| Operating System | Windows 10 Threshold 2 |
| Kernel Version | 10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379) |
| Network Scheme Name | Local Gateway |
| Network Config Name | Local Gateway |

### Platform Information

| | |
|---|---|
| Platform Version | 4.3.0 |
| Dynamic Engine Version | 4.3.0 / 09/20/2021 03:59 |
| Static Engine Version | 4.3.0.0 / 2021-09-20 03:00:12 |
| AV Exceptions Version | 4.3.0.0 / 2021-09-20 03:00:12 |
| Link Detonation Heuristics Version | 4.3.0.4 / 2021-09-16 11:30:34 |
| Signature Trust Store Version | 4.3.0.0 / 2021-09-20 03:00:12 |
| VMRay Threat Identifiers Version | 4.3.1.7 / 2021-09-22 10:00:51 |
| YARA Built-in Ruleset Version | 4.3.0.5 |

### Anti Virus Information

| | |
|---|---|
| Built-in AV Version | AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021) |
| Built-in AV Database Update Release Date | 2021-09-28 08:04:18+00:00 |
| Built-in AV Database Records | 10477558 |

### Software Information

| | |
|---|---|
| Adobe Acrobat Reader Version | Not installed |
| Microsoft Office | 2016 |
| Microsoft Office Version | 16.0.4266.1003 |
| Hangul Office | Not installed |
| Hangul Office Version | Not installed |
| Internet Explorer Version | 11.0.10586.0 |
| Chrome Version | Not installed |
| Firefox Version | Not installed |
| Flash Version | Not installed |
| Java Version | Not installed |

### System Information

| | |
|---|---|
| Sample Directory | C:\Users\RDhJ0CNFevzX\Desktop |
| Computer Name | XC64ZB |
| User Domain | XC64ZB |

| | |
|---|---|
| User Name | RDhJ0CNFevzX |
| User Profile | C:\Users\RDhJ0CNFevzX |
| Temp Directory | C:\Users\RDHJ0C~1\AppData\Local\Temp |
| System Root | C:\Windows |